REMARKS

Claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39 and 41-81 are pending in the present patent application. The Examiner has rejected claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39 and 41-81. Applicant has amended claims 1, 18-19, 32, 36, 41-44, 52-53, 57-58, 60, 62, 68-69, 74, and 79-80. Dependent claims have been amended herein to eliminate 35 USC 112 compliance issue. Applicant respectfully requests reconsideration of claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39 and 41-81 in view of at least the following amendments and remarks.

I. Rejection of Claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39 and 41-81 Based on 35 U.S.C. § 103

The Examiner has rejected claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23, 27, 32-34, 36, 39, 41-56, 58-60 and 68-81 under 35 USC §103(a) as being unpatentable over Kara '739 in view of Talmadge '138. The Examiner states:

> Kara discloses a secure on-line printing method:
>
> establishing a communication link between a first computer and a second computer (*i.e., claim 27, the step of "coupling said first system to a second processor-based system"*);
>
> executing a client software on said first computer, wherein said client software initiates a secure continuous communication link between said first computer and said second computer (*col. 6, lines 11-17; col. 11, lines 6-12 and 18-21*);
>
> sending a request for value bearing information from said client software to said second computer (*i.e., claim 27, the step of "transmitting said demand from said first system to said second system"*); and
>
> sending said value-bearing-information from said second computer to said first computer in response to said request (*i.e., claim 27, the step of "transmitting said data packet from said second system to said first system"*), while said communication link is continuous (*col. 11, lines 13-18*); and printing said value-

bearing information while said secure continuos [sic] communication link persists (*col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia*).

Further, Kara discloses a secure on-line postage metering method comprising:

establishing a secure communication link between a user computer and a vendor computer (i.e., claim 27, the step of *"coupling said first system to a second processor-based system" and using an encryption module*);

providing a printer connected to said user computer (*printer 24*);

executing an on-line postage metering software on said user computer wherein said on-line postage metering software determines if said secure communication link between said first computer and said second computer is continuous (*col. 6, lines 11-17; col. 11, lines 6-12 and 18-21*));

said on-line postage metering software (*i.e., "Demand program"*) sending a request for a print authorization to said vendor computer (*i.e., claim 27, the step of "transmitting said demand from said first system to said second system"*);

said vendor computer accessing a database to verify fund availability to cover said request (*col. 13, lines 31-45*);

said vendor computer sending data elements for a postage indicium to said first computer as a response to said request (*i.e., claim 27, the step of "transmitting said data packet from said second system to said first system"*); and

said on-line postage metering software sending a postage indicium graphic associated with said data elements to said printer while said secure continuous communication link persists (*i.e., "Demand program" decrypting the received data packet for printing and col. 11, lines 6-12 and 18-21*)).

Regarding claim 1:

Kara does not explicitly disclose the steps of monitoring said secure continuous communication link between said first and said second computer and terminating said client software when said communication link is not continuous. However, Talmadge discloses the steps of monitoring said secure continuous communication link between said first and said second computer and terminating said client software when said communication link is not continuous to secure vault having electronic indicia (*e.g., the system having means for disabling the host module from activating the print means to print said indicia unless said vault module is coupled thereto as claim 20 would inherently monitor whether the link between the vault module and the host module is continuous or not*). Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Talmadge to further enhance the security of the claim method.

Regarding claims 3 and 4:

Kara discloses said request and said value-bearing item information comprising encrypted data (*col. 6, lines 17-22*).

Regarding claim 6:

Kara discloses said value-bearing information comprising an image of a postal indicium (*col. 6, lines 40-42*).

Regarding claim 7:

Kara discloses said request comprising a postage amount (*col. 6, lines 4-7*).

Regarding claim 10:

Kara discloses that said sending said request is in response for said value bearing information to a command from a user (*col. 3, lines 16-19*).

Regarding claims 12 and 13:

Kara discloses said second computer comprising a database containing user information, wherein said user information comprises financial information associated with said user (*col. 13, lines 31-45. It is well known in the art to keep user s*[sic] *credit or debit account in a database*).

Regarding claim 14:

Kara discloses said sending said request to said second computer further comprises accessing said user information to verify fund availability to cover said postage amount (*col. 13, lines 31-45*).

Regarding claim 18:

Kara does not explicitly disclose that said value-bearing information comprises disabling the print spooler of a printer connected to said first computer. However, Talmadge discloses the step of disabling the printer connected to said first computer to secure vault having electronic indicia (*e.g., claim 20*). Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Talmadge to further enhance the security of the claimed method.

Regarding claim 19:

Kara discloses that said client software sending a print command to said printer when said communication link disconnects (*e.g., see FIG. 2*).

Regarding claims 20 and 21:

Kara discloses said value-bearing information comprising ticket information and said request comprises a ticket price (*col. 15, lines 27-32*).

Regarding claims 23 and 27:

Kara discloses that said second computer sends authorization to said first computer in response to said request, said second computer accessing said user's financial information to verify funds availability *(col. 13, lines 31-45. If proper*

funding is available, said second computer sends permission to said first computer to use the Meter program).

Regarding claims 32, 36 and 41:

Kara does not explicitly disclose the step of terminating said online postage metering software when said communication link is not continuous, said on-line postage metering software disabling a print spooler of said printer, and said online postage metering software sending a print cancel command to said printer if said secure communication link is interrupted. However, Talmadge discloses the step of disabling the printer connected to said first computer to secure vault having electronic indicia (*e.g., claim 20*). Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Talmadge to further enhance the security of the claimed method.

Regarding claims 33 and 34:

Kara discloses said online postage metering software sending a request comprising encrypting said request and said vendor computer sending said response comprising encrypting said response (*col. 6, lines 17-22*).

Regarding claim 39:

Kara discloses that said on-line postage metering software sending said request for said print authorization is in response to a command from a user (*col. 3, lines 16-19*).

Regarding claim 42:

Kara discloses a secure on-line postage management method comprising:

establishing a secure continuous communication link between a client system and a server system (*col. 6, lines 11-22*);

said client system processing a user request for obtaining an indicium (*col. 6, lines 11-22*);

said client system securely communicating said user request to said server system (*col. 6, lines 11-22*);

said server system processing said user request (*col. 6, lines 37-43*);

said server system securely communicating to said client system a response to said user request (*col. 6, lines 11-22*);

said client system processing said response to obtain said indicium (*col. 6, lines 11-22, "decrypting the received data packet"*);

said client system obtaining said indicium while said secure continuos [sic] communication link persists (*col. 11, lines 6-12 and lines 18-21 and receiving data packet*); and

said client system printing said indicium while said secure continuous communication link persists (*col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia*). See also the rejection "Regarding claim 1:" above.

Regarding claim 43:

Kara discloses that said client system securely communicating with said server system comprises authenticating a user by establishing said secure communication link between said client system and said server system and verifying the authenticity of information exchanged; and continuously monitoring said secure communication link to verify said authenticity of information exchanged (*col. 6, lines 11-22, "utilizing cryptographic key sets"*).

Regarding claims 44 – 53:

Kara states the use of various security processes (col. 6, lines 11-22) without explicit disclosure of the specifically claimed features. However, the examiner takes official notice of both motive and modification necessary for these features. More specifically, these features are well known in the E-commerce art to prevent theft of confidential information (e.g., credit card or debit account number) or fraud. Thus, it would have been within the level of ordinary skill in the art to employ above well-known features for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number) or fraud.

Regarding claim 54:

Kara discloses that said server system processing said user request takes place in a public network (*"the Meter program"*) and a private network (*"the bank card company" of the user*) included within said server system.

Regarding claim 55:

Kara discloses that said public network processes (*"preparing data packet" by the "Meter program"*) user requests independently from a said private network (*col. 13, lines 49-50, "credit account maintained at the local site and transmitted with the indicia request"*) to protect the integrity of said server system.

Regarding claim 56:

Kara discloses that communication between said client system and said server system is encrypted (*col. 6, lines 11-22*).

Regarding claim 58:

Kara does not explicitly disclose the step of disabling said client system from obtaining said indicium if said secure and continuous communication between client system and server system is discontinued. However, the examiner takes official notice of both motive and modification necessary for this feature. More specifically, these features are well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of ordinary skill in the

art to employ these well-known features for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

Regarding claim 59:

Kara discloses that said private network processes said user requests for making payments (*col. 13, lines 49-50, "credit account maintained at the local site and transmitted with the indicia request"*).

Regarding claim 60:

Kara discloses that said private network processes said user requests for making payments further comprises communicating with a financial management system for verification of availability of funds and fund transfer (*col. 13, lines 49-50, "credit account maintained at the local site and transmitted with the India request"*).

Regarding claim 68:

Kara discloses maintaining said continuous communication link between said client system and said server system and retrieving said indicium from said server system (*col. 6, lines 11-22 and lines 39-43*).

Regarding claim 69:

Kara discloses a method having steps of establishing a secure continuous communication link between a client system and a server system (*col. 6, lines 11-17*), wherein said client system comprises client system software (*"Demand" program*); said client system software presenting one or more options for submitting at least one payment (*col. 13, lines 31-45*); submitting said at least one payment to said server system software while said secure continuous communication link persists (*col. 13, lines 25-30 and 31-45*); adding postage value corresponding to an amount of said at least one payment to a user account (*col. 13, lines 25-30 and 31-45, i.e., credit account for later billing*); and printing at least one indicia representative of said postage while said secure continuous communication link persists (*col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia*). See also the rejection "Regarding claim 1:" above.

Regarding claim 70:

Kara discloses the step of deducting said amount from said user account (*col. 13, lines 25-30 and 31-45, i.e., deducted from the user's debit account*).

Regarding claim 71:

Kara discloses that said deducting is performed upon authorization from said user (*col. 13, lines 25-30 and 31-45, i.e., the user supplying certain information about the user's debit account*).

Regarding claim 72:

Kara discloses said at least one payment comprising credit card data (*col. 13, lines 25-30 and 31-50, i.e., bank card*).

Regarding claim 73:

Kara discloses said at least one payment comprising electronic funds transfer data (*col. 13, lines 25-30 and 31-50, i.e., bank card*).

Regarding claim 74:

Kara discloses a computer program product having a computer readable medium having client system software (*i.e., "a data communications program"*) embodied therein, said client system software configured to: establish a secure continuous communication link between a client system and a server system (*col. 6, lines 11-17*) comprising server system software (*i.e., "a meter program"*), wherein said client system comprises client system software (*i.e., "Demand program"*) configured to present one or more options for submitting at least one payment (*col. 13, lines 31-45*); said client system configured to submit said at least one payment to said server system software while said continuous communication link persists between said client system and said server system (*col. 6, lines 11-17; col. 13, lines 25-30 and 31-45, i.e., "a data communication program" processes information*); said server system software configured to credit postage value corresponding to an amount of said at least one payment to a user account (*col. 6, lines 11-17; col. 13, lines 25-30 and 31-45, i.e., "a data communication program" processes information*); and said client system software printing at least one indicia representative of said postage value while said secure continuos [sic] communication link to said server system software persists (*col. 11, lines 6-12 and lines 18-21 and printing the desired postage indicia*). See also the rejection "Regarding claim 1:", above.

Regarding claim 75:

Kara discloses the computer program product comprising said client system software configured to deduct said amount from said user account (*col. 6, lines 11-17; col. 13, lines 25-30 and 31-45, i.e., "a data communication program processes information and deduction from the user's debit account"*).

Regarding claim 76:

Kara discloses that said submitting is performed by said client system software upon authorization from said user (*col. 6, lines 11-17; col. 13, lines 25-30 and 31-45, i.e., the user supplying certain information about the user's debit account and "a data communication program" processes information*).

Regarding claim 77:

Kara discloses said payment comprising credit card data (*col. 13, lines 25-30 and 31-50, i.e., bank card*).

Regarding claim 78:

Kara discloses said payment comprising electronic funds transfer data (*col. 13, lines 25-30 and 31-50, i.e., bank card*).

Regarding claim 79:

Kara discloses that said continuous communication link utilizes Internet protocols to transfer data (*col. 15, lines 19-21*).

Regarding claim 80:

Kara does not explicitly disclose that said client system software prohibits transmission if said secure continuous communication link fails authentication. However, the examiner takes official notice of both motive and modification necessary for this feature. More specifically, this feature is well known in the data processing art to transfer confidential data securely and the failure of authentication signifies that there is a possibility of transferring sensitive data to a wrong place or security breach of the communication link and it would have been within the level of ordinary skill in the art to employ this well known feature for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number)

Regarding claim 81:

Kara discloses data transmitted between said client system software and said server system software comprising encrypted information (*col. 6, lines 17-22*).

The Examiner has rejected claims 24, 25, 28, 29 and 31 under 35 USC §103(a) as being unpatentable over Kara in view of Talmadge as applied to claim 1 above, and further in view of Edelmann et al '246. The Examiner states:

Kara in view of Talmadge discloses the method as stated supra. Further, Kara states that his invention may be utilized to transmit any form of indicia. (Col. 15, lines 25-26) without explicitly disclosing the value-bearing information comprising check information, coupon information or certificate information and the request comprising a check amount or a coupon amount. However, Edelmann shows various forms of indicia (*e.g., postage, parcel service, tax stamps, checks writing, ticket, and other similar indicia: col. 5, lines 17-23*). Thus, it would have been obvious to one of ordinary skill in the art to modify the method of Kara by employing the value-bearing information comprising any known indicia as shown by Edelmann as desired to detect fraudulent imprints on documents that require verification and authentication of a user.

The Examiner has rejected claims 57, 61-67 under 35 USC §103(a) as being unpatentable over Kara in view of Talmadge as applied to claim 42 above, and "Information Based Indicia Program system Specification", USPS, (referred to hereinafter as IBIPSS). The Examiner states:

Regarding claim 57:

Kara discloses the method as stated supra except for explicit disclosure of the secure communication between client system and server system being encrypted by a United Stated Postal Service compliant cryptographic device. However, as shown by IBIPSS (*see page 3-13, section 3.2.6.3*), the open system server shall prompt the user to apply (*register*) for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to employ the client system and server system being encrypted by a United States Postal Service compliant cryptographic device to establish a communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement.

Regarding claims 61 and 62:

Kara does not explicitly disclose that said server system communicating with the United States Postal Service Central Meter Licensing System (USPS (CMLS) for processing of user licensing information. However, as shown by IBIPSS (*see page 3-13, section 3.2.6.3*), the open system server shall prompt the user to apply (*register*) for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to establish a communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement.

Regarding claim 63:

Kara discloses an on-line postage system for processing of user requests and obtaining postage indicia comprising:

a client system (*a first processor-based system*) for interfacing with a user;

a server system (*a second processor-based system*) in continuous and secure communication with said client system, comprising (*col. 6, lines 11-22*):

a communication server for communicating with client system (*col. 7, lines 18-36*);

a database server for storing user information (*col. 14, lines 24-30*);

a transaction server for processing of requests communicated to said server system by said client system (*col. 14, lines*);

a cryptographic device for encrypting communication between said client system and said server system (*col. 6, lines 20-23, i.e., "decrypting the*

received data packet" implies that the second processor-based system must have a cryptographic device);

a continuous communication link with a financial management system for processing user payments (*col. 13, lines 45-50, i.e., "the provider will demand payment from the bank card company concurrent with the postage demand."*).

Kara does not explicitly disclose either a firewall for ensuring the integrity of said server system against potential unauthorized access or a continuous communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user. However, as shown by IBIPSS (*see page 3-13, section 3.2.6.3*), the open system server shall prompt the user to apply for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to establish a continuous communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement. Further, the communication link must be continuous with the USPS CMLS until the licensing of the user is finalized. Still further, Kara states that the server system can be used by a plurality of remotely located client systems and the client system provides security system to prevent unauthorized utilization of the postage metering system (*col. 4, lines 36-51*). Of course, a firewall is one of the well-known security systems in the art and the use of this well known feature at the server system would have been within the level of ordinary skill in the art, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

Regarding claim 64:

IBIPSS disclose the use of a system software down-loadable from said server system to said client system (*see page 3-3, section 3.2.1.1*) to ensure the proper installation and configuration of the user system. Thus, it would have been obvious to one of ordinary skill in the art to modify the system of Kara by adopting the teaching of IBIPSS to ensure the proper installation and configuration of the client system.

Regarding claim 65:

Kara discloses that said client system interfaces with at least one user (*col. 5, lines 65-67*).

Regarding claim 65:

Kara discloses that said server system is accessible through an Internet portal (*col. 7, lines 25-27*).

Regarding claim 67:

Kara discloses that said client system comprises administration software (*i.e., a data communications program*) to monitor (*i.e., to maintaining a link, the data communication program has to monitor the system*) said client system.

Applicant respectfully submits that, as amended, independent claims 1, 32, 42, 63, 69, and 74 are allowable for at least the reasons stated in the response mailed on August 28, 2002 (filed on September 3, 2002), which are herein incorporated by reference.

In addition, Applicant submits that neither Kara nor Talmadge, alone or in combination with any other prior art teaches, suggests, or describe actively printing (e.g., in real-time) the value bearing information only while the secure link between the first computer and the second computer is continuous (see support in specification page 15, lines 19-24, and page 69 line 20 to page 70 line 8). In fact, Kara specifically teaches that the communication link is not needed and may be terminated after the postage indicia is fully received (col. 11, lines 17-18) in the first computer. Thus, in Kara, Talmadge, and other prior arts cited by the Examiner, printing of the indicia is not a condition for sending the indicia from the second computer to the first computer and those prior art systems have no way of coupling the indicia printing process from the first computer with the indicia sending process in the second computer.

Thus, Applicant submits that, as amended, independent claims 1, 32, 42, 63, 69, and 74 are patentably distinct from the prior art thus are in condition for allowance.

Dependent Claims 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31, 33-34, 36, 39, 41, 43-62, 64-68, 70-73, and 75-81

Applicant respectfully submits that claims 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31, 33-34, 36, 39, 41, 43-62, 64-68, 70-73, and 75-81, being dependent upon respective allowable base claims are also allowable for at least the foregoing reasons stated above.

CONCLUSION

For at least the foregoing reasons, Applicant respectfully submits that pending claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39 and 41-81 are patentably distinct from the prior art of record and in condition for allowance. Applicant therefore respectfully requests that pending claims 1, 3, 4, 6, 7, 10, 12-14, 18-21, 23-25, 27-29, 31-34, 36, 39 and 41-81 be allowed.

Respectfully submitted,

THE HECKER LAW GROUP

Date: 6/19/03

By: _____
Obi I. Iloputaife
Reg. No. 45,677

THE HECKER LAW GROUP
1925 Century Park East
Suite 2300
Los Angeles, California 90067
(310) 286-0377

CERTIFICATE OF MAILING

This is to certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Arlington, VA. 22313-1450 on June 19, 2003.

Signature:: Marlou Maglente *Date: June 19, 2003*